Annual ADFSL Conference on Digital Forensics, Security and Law

2010 Proceedings

May 19th, 1:00 PM

Social Networking: A Boon to Criminals

Tejashree D. Datar
Computer and Information Technology Department, Perdue University, tdatar@purdue.edu

Richard Mislan
Computer and Information Technology Department, Purdue University, rick@purdue.edu

Social Networking: A Boon to Criminals

Tejashree D. Datar
Computer and Information Technology Department
401 North Grant Street, Knoy 255
Purdue University
West Lafayette IN 47907-2021
tdatar@purdue.edu

Richard Mislan
Computer and Information Technology Department
401 North Grant Street, Knoy 255
Purdue University
West Lafayette IN 47907-2021
rick@purdue.edu

ABSTRACT

With the world getting more and more digitized, social networking has also found a place in the cyber world. These social networking sites (SNSs) which enable people to socialize, and build and maintain relationships are attracting attention of all kinds of people such as teens, adults, sports persons, and even businesses. But these SNSs are also getting unwanted attention from people like sexual predators, spammers, and people involved in criminal and illegal activities. This paper talks about SNSs and how these sites are exploited for criminal or illegal activity. The SNSs are discussed in detail with respect to user profiles, user networks, and privacy and security with respect to these user accounts. The paper also talks about the way available data on these SNSs can be exploited. The paper concludes with a few real life recent criminal cases associated with these SNSs.

Keywords: social networking, social networking sites, Facebook, MySpace, online predators, phishing, social networking crime, social networking models

1. INTRODUCTION

With the advent of the Internet, it is now very easy to be connected to a number of people, groups, and communities which was not this easily possible before the Internet was widely available. The Internet gave rise to *online* social networking which is mostly done via the use of social networking sites (SNSs) such as Facebook, Twitter, MySpace, Friendster to name a few among the many available SNSs. Today, online social networking has become such a huge phenomenon, that Twitter was declared the most popular English word of 2009 (Parr, 2009). Facebook, one of the social networking sites, ranks third in the overall web traffic in the United States with over 104.2 million users per month (Quantcast, 2009a). MySpace, another social networking site ranks tenth in the overall United States web based traffic with over 55.8 million users per month (Quantcast, 2009b). Online Social Networking has become so much part of our daily lives that it is not uncommon to keep all our contacts posted of what we are doing, if not every minute, but everyday of our life. Social Networking has become a powerful tool for businesses and other things like even the 2008 Presidential Election.

The basic purpose of these SNSs is online interaction and communication and maintaining relationships. SNSs have various models, but the most common model is to present a person's profile and to visualize the person's network of contacts to other people (Gross & Acquisti, 2005). These SNSs allow people to put all kinds of personal information on their website. When people join these social networking sites, they have to create their personal profile. This profile contains information such as name, which could be real or pseudo, date of birth, address, hometown, gender, ethnicity,

religion, spouse's information, workplace details, school details, and the person's personal interest. This profile could also include photographs, videos, and personal messages. Other members can connect by sending friend requests or messages. When a person is added to the contact list or the friend list, this person gets the privilege to access the friend's profile and all the personal information put on this profile. These SNSs also have the privacy option wherein the profile user can hide all of the available personal information from other users except their friends in the friend list, that is, users who are directly connected to the profile owner. Even with all this available privacy, users are least bothered about their profile privacy and are happy to share all the personal information with the online world.

With such personal information as name, address, date of birth, gender, information on children, personal messages like updates, and photos made easily available by the users themselves, it is easy for criminals to gain access to this information. But as per these SNSs models, these criminals also get access to the directly connected contacts of the user. These criminals are commonly referred to as "Online Predators". This paper focuses on three popular social networking sites in the United States, namely, Facebook, MySpace, and Twitter. The paper will describe social networking and its history, and then will describe the above-mentioned three sites in detail concerning the user profile, content, and privacy. It will then describe the possible use of these sites by online predators to conduct their criminal activities.

2. SOCIAL NETWORKING: EVOLUTION

Until the 1990s, Internet was not so widely and commercially available to the common public. As Internet started becoming more available and more popular, people started viewing it as a useful and commercial application. This was the evolution of online social networking. But does it mean that people did not socially connect to each other before the Internet boom? Human being, in itself is called a social animal. Social networks have been studied and analyzed for a long time now. This analysis of social networks is useful in studies of kinship structure, social mobility, science citations, contacts between members of deviant groups, corporate power, international trade exploitation, class structure, and many other areas (Scott, 1998). Internet was a revolution; similar to how telephone was a revolution. As social networking is nothing but maintaining relationships and building new relations, before the advent of the Internet, people used simple methods like snail mail, telegrams, telephones and even actually physically meeting each other to maintain and build new contacts.

In the 1980s and 1990s, a form of social networking called the Bulletin Board System or simply BBS was popular. Here people could send text messages and the BBS ran over the telephone lines (Gigaom, 2008). The first site that could be called as a social networking site came into being in 1997. This was the start of online social networking with SixDegrees.com coming into existence. Users were able to create profiles and list friends using SixDegrees. By 1998, users could also search for friends on SixDegrees. SixDegrees promoted itself as a tool where people could connect with each other and send messages to each other. But SixDegrees failed as a business and in 2000 was finally closed (Boyd & Ellison, 2007). In 2002, social networking sites finally started blossoming with the introduction of Friendster. MySpace was introduced in 2003, while Facebook was open to the general public in 2006. Twitter was also launched in 2006 (Nickson, 2009). Thus started a new age of social networking that we have now come to know.

3. USER PROFILE CONTENT OF THE SOCIAL NETWORKING SITE

As stated earlier, this paper concentrates on the three most popular social networking sites in the US, namely, Facebook, MySpace, and Twitter. An account was specifically created for the purpose of this paper on each of these sites. While Facebook and MySpace have more fields as compared to Twitter, all these sites ask for information like name, birth date, photograph, hometown to just name a few. Compared to Facebook and MySpace, Twitter has more concentration on "chat" for social networking. Facebook and MySpace are more oriented towards maintaining and building new relationships. The

amount of personal information that could be put up while creating a user profile on Facebook and MySpace is astounding. Apart from the fields mentioned earlier, a user could put in information like gender, sexual orientation, relationship status, movie or music taste, biological data to name a few. Appendix 11.1 lists and compares all the available fields related to a user profile on all the three sites.

With all this data relating to personal information available on the Internet, privacy is now a huge concern. Most of the user profile fields on these sites have an option of visibility. This means that the user can decide if the specific content should be available to everyone on the network (here network means the entire SNS network) or just the user's personal network of friends. Even with all this form of privacy available, users tend to keep their profiles open to everyone. This has created a huge security concern as crimes related to these SNSs started rising. These crimes could be anything from cyberstalking, social phishing to sexual assault. These sites are even referred to as "Predators Playground" (Schrobsdorff, 2007).

4. OPERATION OF THE SITES AS A SOCIAL NETWORK

Social networking works in the same way as computer networks. One user is directly connected to a number of users namely contacts or friends and these friends are in turn connected to other contacts. This forms a kind of web or mesh where users act as nodes and every node has multiple branches, which are the user's contacts.

Since every user on these SNSs is unique, the amount of information put out by each user is different. The way these users behave online is hard to define, but this behavior generates out of trust. Fukuyama, and Lewis and Weigert in their respected papers (as cited in Dwyer, Hiltz, & Passerini, 2007) discuss that trust is a critical determinant in personal or face to face relationships. Similarly, Coppola, Hiltz, and Rotter, Jarvenpaa and Leidner, Meyerson, and Piccoli and Ives in their respective papers (as cited in Dwyer, Hiltz, & Passerini, 2007) discuss that trust is also important for successful online interactions. Metzger in her paper write that(as cited in Dwyer, Hiltz, & Passerini, 2007) trust is a precondition for disclosure in interpersonal exchange situations, because of the reduced perceived risks which are involved while revealing private information (Dwyer et al. 2007).

From the above arguments it can be said that relationships on these sites will not be built without trust. To build up a relationship, the user generally adds other users as their friends only if they know each other, even though it was a very brief interaction. The way these SNSs' networks work, once a person is being added into the friend list, this person can access all the information of the user including the users other contacts. This way, it will not be very difficult for an online predator to gain trust of an individual by employing the briefest of interactions and once added to the friend/contact list, exploit this individual's personal data and also maybe search for other potential victims through the now open medium of "Friend List". Crime via social networking is increasing rapidly and criminals are now viewing these SNSs as a tool for committing crimes. If the user account is not open to everyone, the key point of the user information being available for exploitation lies in gaining trust and access to the user profile via Friend/Contact List.

5. FINDING THE USER INFORMATION FOR EXPLOITATION

There are many ways of finding the user information. The user itself can be found by doing a simple search in search engines like Google or Bing. There are certain privacy features available for users of the SNSs that allow the users to not be found via the search engines. This is called profile searchability. Online predators do not search explicitly for users this way. They prefer to contact potential targets as a user of the SNS. Wolak, Finkelhor, and Mitchell in their paper write that online predators prefer to meet and seduce their victims online. They also say that majority of the victims are aware that they are conversing with an adult (Wolak et al. 2008). In a social phishing study conducted by Jagatic, Johnson, Jakobsson, and Menczer, they found out that students readily give university information to a non-university party. They say that a phisher can mine information about relationships via social networking sites. For this study, Jagatic, Johnson, Jakobsson, and Menczer

used freely available user profile data from SNSs for the phishing attack. This data appeared to originate from a friend on the network. They found that the targets were much more likely to disclose personal information to friends than strangers (Jagatic et al. 2005).

So how much information is easily available? Acquisti and Gross in their study found that Facebook users have more trust in the Facebook privacy settings. These users are not much concerned about the information in itself as they think that they can control the information and the privacy controls as to who can view the data. They found out that users are also mildly concerned about who can access their personal data. Another interesting thing Acquisti and Gross found in their study was that users of Facebook, trusted the system and its members more than compared to MySpace (Acquisti & Gross, 2006).

With the users having this attitude towards privacy and trust, with respect to both the SNS and the users in the contact list, it is very easy for online predators to gain access to personal information of the users or for phishers to use phishing methods to collect personal data.

6. PRIVACY AND SECURITY

SNSs have a lot of privacy features. Users have control over who can search their profile called the profile searchability or who can view their profile called profile visibility. A user's direct network of contacts has exclusive privilege of viewing all of the users content such as the message posts by the user and by user's other contacts on the user's profile. These direct contacts have access to all of the user's photos, videos, list of the communities, friend/contact lists. These users however, cannot see the messages/mail communication between the user and the user's other contacts.

The privacy issue arises when some user content is seen or accessed by unintended people. This occurs when "friends of friends" or secondary contacts can view the user's content like photos, and videos. A user can be connected to thousands of secondary users or the friends of friends and this potentially increases the risk of personal information being available to users who are not even in the contact/friend list of the user. Acquisti and Gross in their paper write that an online social network lists hundreds of direct contacts/friends and include hundreds and thousands of additional contacts which are just three degrees of seperation from the subject (Gross & Acquisti, 2005).

With these statistics it is very easy to cross reference a particular user via the open friends/contacts channel. If an online predator gained the trust of a teen and gets added to that teen's contact/friend list, this opens a big window for this online predator to search for potential victims via this teen's friend/contact list. This predator will also have access to the teens photos and from there access to any open profiles as well as photos, videos, and personal information of the teen's other contacts, which essentially become the predator's secondary contacts.

Phishers work in different way. They gain unauthorized access into a users account and start sending spam to the user's direct contacts. These messages could be anything like the Nigerian Scam or appear to come from the user and ask to fill information on a third party network or could be even a virus which infects the machine if the link to it is clicked. SNSs are opening new doors for phishers and scammers. One can become a member of these SNSs very easily. Also, most of these sites lack basic security measures like SSL logins. This makes it easy for hackers to access the user data without the site's direct collaboration (Gross & Acquisti, 2005).

7. EXAMINING THE SNSS FOR INVESTIGATIVE PURPOSES

With the vast amount of data that is readily available on the SNSs, similar to criminals, investigators can also use this data for investigative purposes. The ways of finding user information for investigative purposes is very much similar to what the criminals use. For investigative purposes, a specific user will be targeted to gather information from. Shoemaker in her paper (as cited in Lampe, Ellison & Steinfield, 2006) write about a function called 'surveillance' which allows an individual to track the actions, beliefs and interests of the larger group, to which they belong to (Lampe et al. 2006).

Lampe et al. classified this type of surveillance by the goals of users as 'social searching' or 'social browsing'. Social searching is where the site is specifically used to investigate specific people. Social browsing helps to find people or groups with whom the individual wants to connect offline (Lampe et al. 2006). Social searching is the type of surveillance that investigators use as they target specific individuals to gather information.

Just like normal people, criminals tend to keep their profiles open to public. Some criminals go as far as to put status updates about the crimes they have commited. Investigators can use these SNSs to verify an alibi, or to even just check up the profile of the particular individual. SNSs are used by the investigators as form of resource. They use these sites more reactively rather than proactively (Klein, 2008). Apart from investigators, people like insurance adjustors, insurance attorneys, prosecutors, defense attorneys are also taking help of the SNSs to check out their clients or their witnesses (McKinney, 2010).

8. SOME CYBER CRIME CASES INVOLVING THE SNSS

With the increase in popularity of the SNSs among general public, there is also an increase of popularity of these SNSs among criminals. These SNSs have actually opened a lot of doors for the crime world and the ways the crime is committed. Now-a-days, reports of lot of criminal activities involving the SNSs can be heard. Facebook and MySpace are especially popular in this area. A few cases relating to SNS are listed below.

Recently in the news was John Forehand, who was arrested for allegedly asking his teen daughter for sex over Facebook. John Forehand started communicating with his teen daughter over Facebook. He then told her that he was having inappropriate dreams about her and then proposed sex with her via posting graphic details of the activity on her Facebook account (The Huffington Post, 2009). In this particular case, the teen daughter added John Forehand to her contacts/friend list, as she must have trusted him since he was her father. If we can call John Forehand a predator, then the daughter's other teen contacts could be considered potential victims. John Forehand had easy entry in any open accounts via his daughter's contact/friend list.

In another case, a man named Robert A. Wise was arrested on charges of online solicitation of a minor. Wise was sending explicitly sexual messages to a teenage girl via MySpace. After being contacted the police posed as the 14 year old girl on MySpace and via the MySpace chat arranged a meeting with him. When Wise came to meet the girl at a prearranged spot, he was arrested. The cops also found online evidence against Wise to charge him with the sexual assault of another 14-year-old girl he had allegedly met on MySpace (Schrobsdorff, 2007). In yet another case a Houston man was arrested with sexual assault of a child. This 15 year old teen had been communicating with this man on MySpace and had actually snuck out of the house to meet him in person (Schrobsdorff, 2007).

In yet another incident, Emily Mayhan, a 20 year old Facebook user found that her Facebook account had been hijacked and the password to the account changed due to which she could not access the account. After that several of the contacts in her friend list started getting messages stating that she was stranded in London without cash and in urgent need of cash. Facebook closed her account on account of suspicious activity after a few days but no action was taken on the incident. According to the Federal Bureau of Investigation (FBI), this is a case of online hoax or phishing, which takes place for identity theft or for financial information (Davis, 2009).

In yet another phishing scam on Facebook, Bryan Rutberg's Facebook account had been hacked into and messages appearing from him were being posted saying that he is in urgent need of help. Many of his contacts also received emails saying he had been robbed at gunpoint while travelling in the United Kingdom and he was in need of money. Rutberg was locked out of his own account and the scammer had even removed his wife from his contact list. The account was de-activated after about 24 hours (Sullivan, 2009).

And lastly but not the least, "Spam King" Sanford Wallace was sued by Facebook for accessing users'

accounts without their permission and then sending phony messages and posts. Facebook claimed that Wallace used phishing sites or other similar means to fraudulently gain access to Facebook accounts of the users. After that, he used these accounts to distribute phishing spam throughout the network (cnet, 2009). Wallace was also charged and fined for the MySpace case in 2008 where he sent junk messages to the MySpace users (USA Today, 2009).

9. CONCLUSION

While social networking sites are a good way of maintaining relationships and building new relationships, a user should be always aware of the existing dangers of using these sites. With the high amount of personal data put on these sites, there is always a risk of this data being exploited. Even with the use of privacy settings, the data is easily accessed through an open account or even through a closed account. Howsoever innocent the personal data is, online predators are always watching and users are targeted via phishing.

10. REFERENCES

(2009a), 'Profile of Facebook.com', Retrieved from Quantcast: http://www.quantcast.com/facebook.com, November.

(2009b), 'Profile of MySpace.com', Retrieved from Quantcast: http://www.quantcast.com/myspace.com, November.

(2009), *Social Networks, from the 80s to 00s*. Retrieved from Gigaom: http://gigaom.com/2008/01/20/social-networks-from-the-80s-to-the-00s/, November.

(2009), 'John Forehand: Man 'Asked Teen Daughter For Sex On Facebook' (PHOTOS, VIDEO)', Retrieved from The Huffington Post: http://www.huffingtonpost.com/2009/10/12/john-forehand-man-asked-d_n_317148.html, October 12.

(2009), 'Web marketer ordered to pay Facebook $711M damages', Retrieved from USA Today: http://www.usatoday.com/tech/hotsites/2009-10-30-spammer-facebook-damages_N.htm, October 30.

Acquisti, A. & Gross, R. (2006). *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, Retrieved October 2009 from http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf*

Boyd D. M. & Ellison N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication* , *13* (1), Article 11, Retrieved from http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

Davis, M. T. (2009), 'Online Predators turn to Facebook', Retrieved from Missourian: http://www.columbiamissourian.com/stories/2009/10/26/social-network-identity-theft-rise/, October 26.

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). *Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace*. *Thirteenth Americas Conference on Information Systems*. Keystone, Colorado, August 10-12.

Gross, R., Acquisti, A. (2005, Novebmer 7). Information Revelation and Privacy in Online Social Networks (The Facebook Case), Retrieved from http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf

Jagatic T., Johnson N., Jakobsson M., and Menczer F. (2005). Social Phishing. *Communications of the ACM* , Forthcoming (2009).

Klein J. (2008), 'Police: Criminal evidence can be drawn from Facebook, MySpace', Retrieved from Gateway: http://media.www.unogateway.com/media/storage/paper968/news/2008/03/25/NationalNews/Police.Criminal.Evidence.Can.Be.Drawn.From.Facebook.Myspace-3280666.shtml, March 25.

Lampe C., Ellison N., and Steinfield C. (2006). A face(book) in the crowd: social searching vs. social browsing. In *CSCW '06: Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work*, pages 167-170, New York, NY, USA. ACM.

McKinney R. (2010), How Facebook and Social Media Impacts your Case [Video File]. Video Posted to: http://www.nashvillecriminallawreport.com/2010/04/articles/evidence-and-procedure/how-facebook-and-other-social-media-impacts-your-case/

Mills, Elinor (2009), ‘’Spam king’ could face criminal charges in Facebook case’, Retrieved from cnet: http://news.cnet.com/8301-1009_3-10264069-83.html, June 12.

Nickson, C. (2009), ‘The History of Social Networking’, Retrieved from Digital Trends: http://www.digitaltrends.com/features/the-history-of-social-networking/, Janurary 21.

Parr, B. (2009), ‘Twitter Declared Most Popular English Word of 2009’, Retrieved from Mashable The Social Media Guide: http://mashable.com/2009/11/29/twitter-most-popular-word/, November 29.

Schrobsdorff, S. (2007). ‘Predators Playground?’, Retrieved from Newsweek: http://www.kidsafecyberspace.com/wp-content/uploads/2009/07/Predators-Playground.htm, October 15.

Scott, J. (1998). Social Network Analysis. *Sociology , 22* (1), 109-127.

Sullivan, B. (2009), ‘Facebook ID theft targets ‘friends’’, Retrieved from http://redtape.msnbc.com/2009/01/post-1.html, November.

Wolak J., Finkelhor D., Mitchell K. J., Ybarra M. L. (2008). Online "Predators" and their Victims. *American Psychologist , 63* (2), 111-128.

11. APPENDIX

11.1 User Profile Fields for Facebook, MySpace, and Twitter

Facebook	**MySpace**	**Twitter**
Name/alias	Name/alias	Name/alias
Photograph	Photograph	Photograph
Networks		Lists
Sex	Sex	
Birthday	Birthday	
Sexual orientation	Sexual orientation	
Hometown	Hometown	Location
Relationship status	Relationship status	
Friends list	Friends List	Followers/Following/Lists
Political views		
Religious views	Religious views	
Activities		
Interests		
Musical taste	Musical taste	
Television taste	Television taste	
Movie taste	Movie taste	
Books taste	Books taste	
Quotations		
Email address(es)		Email address
Telephone number(s)		
Instant messenger ID(s)		
Educational history	Educational history	
Employment history	Employment history	
Group affiliations	Networking Categories	
Photo albums	Photo albums	
	Blog entries	Link to online Bio
	Personal 'about me' entry	
	Personal heroes	
	'Who I'd like to meet'	
	Zodiac sign	

	Parental status	
Online status	Online status	
Chat 'wall', including time of post	Chat 'comments', including date and time of post	Chat 'tweets', including date and time of post
	Income	
	Country	
	Postal Code	
	State	
Videos	Videos	
	Intentions (dating, relationships, friendship, networking)	
	Height	
	Body Type	
	Drinker	
	Smoker	
	Ethnicity	
		Time Zone

11.2 Some Recommended Safety Guidelines for Users of SNSs

- Always be aware that any content once put on the Internet always stays there even though it appears to be deleted.
- Always be aware of the content put out on the SNSs.
- Always use the available privacy features on the SNS. Do not leave the user profile open to be accessed by everyone.
- Do not accept friend/contact requests from unknown people.
- Think twice before putting any information on the SNSs.
- Avoid putting photos that might attract unwanted attention from any online predators.
- Avoid putting detailed information of oneself as well as family members like spouses, children, and parents.
- Be aware of any phishing content that might appear to be posted by any of the friends.
- Always be aware of the risks of social networking and different uses of SNSs.